No. 23-13698

UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

COIN CENTER *et al.*,
Plaintiffs-Appellants,

v.

SECRETARY, U.S. DEPARTMENT OF THE TREASURY *et al.*,
Defendants-Appellees.

Appeal from the United States District Court
for the Northern District of Florida

BRIEF OF ANDREESSEN HOROWITZ AS AMICUS CURIAE IN SUPPORT OF APPELLANTS AND REVERSAL

Alessio D. Evangelista
Jessie K. Liu
SKADDEN, ARPS, SLATE
MEAGHER & FLOM LLP
1440 New York Avenue, N.W.
Washington, DC 20005
Telephone: (202) 371-7000
Fax: (202) 661-9170
alessio.evangelista@skadden.com
jessie.liu@skadden.com

Counsel for Amicus Curiae Andreessen Horowitz

No. 23-13698
(*Coin Center v. Secretary, U.S. Department of the Treasury*)

CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT

Pursuant to Eleventh Circuit Rule 26.1, counsel for Amicus Curiae certifies that, in addition to the persons and entities listed in Appellants' Certificate of Interested Persons and Corporate Disclosure Statement, the following have an interest in the outcome of this appeal:

1. AH Capital Management, L.L.C. (d/b/a Andreessen Horowitz), *Amicus Curiae*

Amicus Curiae, by and through its undersigned counsel, hereby certifies that a16z Holdings, L.L.C. is the parent corporation of AH Capital Management L.L.C. (d/b/a Andreessen Horowitz), and no publicly held company owns 10% or more of AH Capital Management, L.L.C. (d/b/a Andreessen Horowitz).

December 21, 2023

Respectfully submitted,

/s/ Alessio D. Evangelista
Alessio D. Evangelista

Counsel for Amicus Curiae
Andreessen Horowitz

TABLE OF CONTENTS

TABLE OF CITATIONS

CASES

STATUTES

RULES AND REGULATIONS

OTHER AUTHORITIES

IDENTITY AND INTEREST OF AMICUS CURIAE[1]

Amicus curiae Andreessen Horowitz ("a16z") is a venture capital firm that invests in start-up to late-stage technology companies across a range of sectors, including the blockchain ecosystem. This ecosystem has grown rapidly since it was first developed in 2008. To date, amicus's dedicated funds have raised more than $7.6 billion to invest in companies within this ecosystem. Amicus has been at the forefront of advancing the industry through investments in companies that build blockchain-based solutions relating to identity management, enterprise management, content creation, environmental protection, data storage, and many other sectors. Amicus has significant expertise relating to the unique attributes of crypto assets and decentralized systems and employs a dedicated team of engineers and scholars in these fields.

Amicus's longstanding participation in the blockchain ecosystem supports its strong interest in the law relating to blockchains. For the first time, decentralized blockchain-based protocols allow everyday users and creators greater access, ownership, and control of their data, activities, and actions on the Internet, rather

---

[1] All parties have consented to the filing of this brief. No party's counsel authored this brief in whole or in part, no party or party's counsel contributed money that was intended to fund preparing or submitting the brief, and no person—other than the amicus curiae, its members, or its counsel—contributed money that was intended to fund preparing or submitting the brief.

than having to rely on centralized protocols that give this power to large, third-party corporate entities. That newfound freedom is now threatened, as the Office of Foreign Assets Control ("OFAC") has applied its powerful sanctions authority to effectively disable decentralized, open-source, and ownerless software that was used by thousands of users to add a layer of privacy to their crypto asset transactions. Amicus has a particularly strong interest in this case because decentralized software is a foundational technology in the development of the Internet.

OFAC's decision to sanction Tornado Cash, and the district court's ruling upholding OFAC's action, raise serious, far-reaching legal questions that not only affect amicus's portfolio companies, but also the blockchain ecosystem far beyond this case, including companies that develop decentralized protocols and the applications that developers build on top of them. For this reason, amicus respectfully offers this brief to assist the Court in understanding decentralized software and the significant statutory deficiencies inherent in OFAC's application of sanctions against Tornado Cash.

STATEMENT OF THE ISSUE

Whether the district court erred in upholding OFAC's designation of Tornado Cash, where the sanctioned smart contracts are open-source, decentralized, and ownerless software code, and OFAC's decision will undercut fundamental privacy interests and stifle critical innovation.

SUMMARY OF THE ARGUMENT

This case presents a complex question at the intersection of emerging technologies and the government's power to impose economic sanctions. OFAC's use of its sanctions authority against the Tornado Cash software is the first time that open-source, decentralized, and ownerless software code has been the target of U.S. sanctions. To justify this novel application of sanctions, OFAC relies on two statutes: (1) the International Emergency Economic Powers Act, which empowers the Executive to address national emergencies by blocking "transactions involving[] any property in which any foreign country or a national thereof has any interest," 50 U.S.C. § 1702 (a)(1)(B), and (2) the North Korea Sanctions and Policy Enhancement Act, which provides supplemental authority for blocking "all transactions in *property* and *interests in property* of a person designated" for engaging in certain activities involving North Korea, 22 U.S.C. § 9214(c)(1) (emphases added); *see also* 22 U.S.C. § 9214(c)(2); 31 C.F.R. § 578.802 (OFAC's Cyber-Related Sanctions Regulations); 31 C.F.R. § 510.802 (North Korea Sanctions Regulations). OFAC sanctioned Tornado Cash [2] pursuant to these statutes and the corresponding Executive Orders and regulations.

---

[2] The exact targets of OFAC's sanctions are the "tornado.cash" website and specific "digital currency addresses" available at https://rb.gy/jrwc7.

Critically, as noted above, OFAC's sanctions authority extends only to "property." But the district court completely ignored this statutory requirement, absolving OFAC of the burden to establish that the sanctioned smart contracts qualify as "property" under the governing statutes. Instead, the district court considered only whether any person has an "interest" in the smart contracts. The district court's unjustified disregard of a fundamental statutory limitation on OFAC's power to sanction risks dramatically broadening the scope of OFAC's authority in a way that Congress neither contemplated nor intended. This Court should make clear that every OFAC designation must satisfy each part of the statutory standard, including the definition of "property."

Here, consideration of the "property" prong of the applicable statutes establishes that OFAC's designation of Tornado Cash exceeded its authority. This is because the applicable statutes do not authorize the sanctioning of open-source, decentralized software that is not owned by anyone. While amicus understands and supports the government's desire to neutralize North Korea's ability to launder the proceeds of illicit activity that support weapons proliferation activities, it cannot do so by exceeding its statutory authority. In this instance, OFAC has overstepped its statutory authority in violation of Administrative Procedure Act ("APA") in a fundamental way.

A foundational characteristic of property is that someone must be able to own it. But here, certain targets of OFAC's sanctions cannot be owned. These particular sanctioned "smart contracts"—i.e., lines of open-source, computer code—are immutable and ownerless. Their technical specifications, embedded in code, preclude persons or entities from altering or removing them from the Ethereum blockchain. What is more, no individual will *ever* be able to alter or remove these sanctioned Tornado Cash smart contracts.

In sum, OFAC exceeded its statutory authority and violated the APA when it sanctioned decentralized, self-executing, open-source, and ownerless software. The district court's opinion, if allowed to stand, will undermine perfectly legitimate and laudable efforts to safeguard private citizens' financial privacy through the use of crypto. The district court's decision also risks jeopardizing investment and development in the blockchain ecosystem—and beyond—for fear that years of work could be nullified by a designation unmoored from statutory text and divorced from common understandings of fundamental legal principles. The thousands of users affected by OFAC's sanctions are depending on this Court to overturn the district court's flawed judgment and invalidate the challenged actions. It is the sole prerogative of Congress to expand OFAC's authority, and it has not done so. For these reasons, and as outlined further below, this Court should reverse the judgment of the district court.

ARGUMENT

I. THE PRECISE NATURE OF THE UNDERLYING TECHNOLOGY IS CRUCIAL TO THIS COURT'S REVIEW OF THE DISTRICT COURT'S DECISION.

A proper understanding of the technology underpinning blockchains and crypto is critical to appreciating OFAC's regulatory overreach in this case and the district court's flawed ruling.

A. The Ethereum Blockchain Is a Public Decentralized Network.

As a threshold matter, a blockchain is simply a network of computers on the Internet. Ethereum is a blockchain network that enables peer-to-peer digital interactions to generate a shared world computing platform that can flexibly and securely run any software application users want to code.[3] The Ethereum blockchain works in a distributed manner to create a public database of information, which includes financial transactions. Each transaction completed on the Ethereum blockchain is recorded and posted on its database, or transparent public ledger, which anyone can view from a computer.[4] *See* District Court ECF No. 9, First Am.

---

[3] *See* Vitalik Buterin, *Ethereum*, Coin Center (Mar. 9, 2016), https://rb.gy/j52lb; *see also* First Am. Compl. ¶¶ 2, 41.

[4] Blockchains are also commonly referred to as "public ledgers" because much of the data, though not all, on them relates to financial transactions (and, as explained below, the information in those ledgers is accessible by anyone with an internet connection). *See Blockchain Technology Explained in Simple Terms*, WorldCoin, https://rb.gy/43w8d.

Compl. ¶ 43. This aspect of the Ethereum blockchain is similar to a bank's ledger used to record transactions, but with a critical difference. Traditional bank ledgers, for example, are centralized, private, and modifiable. Most blockchains, on the other hand, are decentralized, public, and unchangeable. The default of the Ethereum blockchain, for instance, is transparency, and every transaction that occurs on it is publicly viewable and irreversible. As a result, an Ethereum blockchain address's entire transaction history on that network is viewable to anyone with access to an Ethereum block explorer website.[5] *See* First Am. Compl. ¶ 3. Because of the public nature of the Ethereum blockchain, there are several methods, described below, in which the identities of people behind transactions can be revealed, along with their cryptographic addresses, transactions, and assets.

Ethereum's network also enables developers to build applications on top of it and allows users to hold and transact assets, create and share content, and communicate over the network without third-party intermediaries. Ethereum is

---

[5] Block explorers are sometimes called the "search engines of Web3," because their features are similar to standard Internet explorers. For example, a Bitcoin block explorer provides data on the Bitcoin blockchain network activity. Anyone on a blockchain explorer could paste a wallet address to view the associated wallet's current holdings and historical transaction data. *What is Etherscan, and What are Block Explorers?*, WorldCoin (Sept. 4, 2023), https://rb.gy/dfra9v; *see also, e.g.*, https://etherscan.io/ (last visited Dec. 21, 2023).

decentralized, meaning that no person, company, or institution, such as a bank or other financial services company, needs to serve as a conduit between parties that interact with one another on the network.

Ethereum provides numerous benefits to its users. Because the Ethereum blockchain does not require any third-party intermediaries, transactions can occur at any time of day or night, are generally settled faster than non-blockchain-based transactions, and are secured through the use of cryptography rather than through a trusted third party. The Ethereum blockchain and the smart contracts operating on it provide safe, low-cost access for people with an Internet connection to conduct secure transactions.

B. The Tornado Cash Smart Contracts at Issue Preserve Privacy and Cannot Be Owned or Controlled by Anyone.

Despite blockchain's benefits, the only privacy protection for most blockchain users, including Ethereum users, is the pseudonymity of users' accounts. Specifically, the "accounts" listed on the Ethereum blockchain are not associated with the actual names or other personal information of Ethereum users, but rather with algorithmically generated "addresses."[6] A cryptographic address is akin to a user name, email address, or phone number, depending on its function. Ethereum

---

[6] An Ethereum address, for example, looks like this: 0x165CD37b4C644C2921454429E7F9358d18A45e14.

users who transfer crypto assets—for instance, Ether (abbreviated as ETH), the cryptocurrency native to the Ethereum blockchain—use such a public-facing address. *See, e.g.*, First Am. Compl. ¶¶ 2, 45. But the pseudonymity of an Ethereum address is rarely sufficient to preserve a user's privacy and prevent a network observer from connecting a public address with a real-life identity. Once a user interacts with another person or entity, the user's entire on-chain transaction history is exposed, and their identity potentially revealed, because it can be traced back from the known public address. *Id.* ¶ 45. Indeed, there is a plethora of individuals and companies with expertise in conducting blockchain analytics to overcome cryptocurrency address pseudonymity.[7]

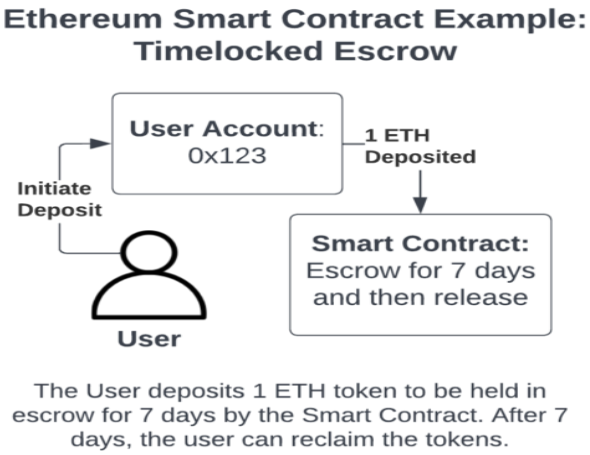
To combat the risk of identity and financial transaction history exposure, many users of Ethereum turn to privacy tools such as the Tornado Cash smart contracts. Privacy-preserving technologies like Tornado Cash emerged as effective solutions to the problem of protecting user anonymity. Tornado Cash smart contracts are a public, open-source software tool. All smart contracts are, essentially, software available to any member of the public on certain blockchains.[8] First Am.

---

[7] Liam Glennon et al., *The Power of Analytics in the Digital Asset Economy*, Accenture (Aug. 23, 2022), https://rb.gy/hznkj.

[8] *See Introduction to Smart Contracts*, Ethereum (Sept. 1, 2022), https://rb.gy/eaadm; Alex Wade et al., *How does Tornado Cash work?*, Coin Center (Aug. 25, 2022), https://rb.gy/ht0d3.

Compl. ¶ 47. The computer code that underlies smart contracts automatically executes all or part of an operation for a user, and when developers program and configure smart contracts, they decide which operations the smart contract will support and which rules those operations must follow.[9]



Source: Wade, *supra* n. 8.

Certain Tornado Cash smart contracts, known as "pool" contracts, create the privacy-preserving function. Specifically, the smart contract pools allow users to deposit crypto assets from one address and later withdraw the same amount from a different address.[10] In so doing, the smart contracts use zero-knowledge proofs that

---

9 *See* Stuart D. Levi and Alex B. Lipton, *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*, Harvard Law School Forum on Corporate Governance (May 26, 2018), https://rb.gy/ycpl9.

10 *Id.*

verify the transaction without leaking specific details of the transaction. A zero-knowledge proof is a cryptographic method whereby "one can prove possession of certain information, e.g., a secret key, without revealing that information, and without any interaction between the prover and verifier." A.R. 34 n. 41; *see also* A.R. 553. Although these Tornado Cash transactions are publicly viewable on Ethereum's blockchain, these transactions are not linked to the user, which ensures the user's privacy and shields the user's financial history from prying eyes.

Importantly, certain sanctioned Tornado Cash smart contracts are completely autonomous. In other words, no individual owns them, and there is no "operator" controlling or altering them. While the code that comprised the initial Tornado Cash software gave its developers certain control over the smart contracts, the developers' goal at the time was to transition particular smart contracts to full decentralization that would allow them to function without an operator, which the developers achieved in May 2020.[11] As a result, transactions occur through those smart contracts autonomously, through self-executing code, and without the assistance of intermediaries. *See* First Am. Compl. ¶ 48. The code for core Tornado Cash smart

---

[11] Tornado Cash, *Tornado.cash version 2 has been released*, Medium (Dec. 17, 2019), https://rb.gy/bkrrf; William Foxley, *Developers of Ethereum Privacy Tool Tornado Cash Smash Their Keys*, CoinDesk (May 18, 2020), https://rb.gy/o5x6f.

contracts (i.e., the Tornado Cash pools) is viewable on GitHub,[12] a free, publicly available website popular with software developers, as well as on the blockchain explorer Etherscan. Anyone with an Internet connection can view, copy, and use the code. In addition, the smart contracts that make up the Tornado Cash software protocol are immutable, meaning that the contracts cannot be altered or removed. *See* A.R. 2146. Finally, Tornado Cash is non-custodial, meaning that Tornado Cash users retain ownership and control of the crypto assets they send to Tornado Cash smart contracts, so neither the smart contracts nor anyone else associated with Tornado Cash takes custody of the users' funds. *See* A.R. 551; First Am. Compl. ¶ 50.

C. Cryptocurrency Is Overwhelmingly Used for Lawful Purposes.

Although OFAC's designation that gave rise to this litigation stems from the use of crypto assets to facilitate criminal conduct on behalf of North Korea, it is essential to remember that the vast majority of crypto transactions, like the vast majority of crypto users, are law-abiding. Indeed, one recent analysis concluded that "the share of illicit [crypto] transaction volume is less than 1 percent."[13]

---

12 *Tornado Cash*, GitHub, https://github.com/tornadocash (last visited Dec. 21, 2023).

13 Norbert Michel, *New Anti-Crypto Movement Escalates Congress's Assault on Privacy*, Forbes (Aug. 2, 2023), https://www.forbes.com/sites/digital- *(cont'd)*

In addition to the countless private citizens who use blockchain technology for non-financial purposes, transact in crypto to safeguard their financial privacy, *see infra* pp. 20–25, or invest in crypto as a means of wealth generation, this technology offers additional benefits for law-abiding individuals and societies at large. For example, "[t]he decentralized nature of crypto allows digital currencies to be traded quickly, making them a useful tool for getting money into conflict and disaster zones."[14] Indeed, the Ukrainian war effort has benefited greatly from crypto, having received over $212 million worth of crypto in support of efforts to repel Russia's invasion.[15] Likewise, "[t]he crypto community raised millions of dollars in donations" in the aftermath of the destructive February 2023 earthquake in Turkey and Syria, "offering a real-time financial lifeline in a situation where traditional banking operations were affected."[16]

---

assets/2023/08/02/new-anti-crypto-movement-escalates-congresss-assault-on-privacy/?sh=333c9c122509.

14 Spencer Feingold, *Why the Role of Crypto is Huge in the Ukraine War*, World Economic Forum (Mar. 16, 2020), https://www.weforum.org/agenda/2023/03/the-role-cryptocurrency-crypto-huge-in-ukraine-war-russia/.

15 *Id.*

16 Aytug Goksu & Busra Kamiloglu, *Turkiye-Syria Earthquake: How AI and Emerging Tech Are Helping Relief Efforts*, World Economic Forum (Feb. 18, 2023), https://www.weforum.org/agenda/2023/02/turkiye-syria-earthquake-ai-emerging-tech-relief-efforts/.

Particularly given crypto's demonstrated record of providing benefits to individuals and societies alike, governments should ensure that the regulation of crypto does not address the small minority of illegal activity at the expense of the vast majority of lawful and responsible uses.

II. THE DISTRICT COURT WRONGLY CONCLUDED THAT OFAC'S SANCTIONING OF TORNADO CASH FALLS WITHIN OFAC'S STATUTORY AUTHORITY.

"Administrative agencies are creatures of statute. They accordingly possess only the authority that Congress has provided." *NFIB v. Dep't. of Lab.*, 595 U.S. 109, 117 (2022). Here, OFAC's application of sanctions to open-source, decentralized, and ownerless Tornado Cash smart contracts is unprecedented and a unilateral expansion of the Executive Branch's power beyond what Congress has granted.

The International Emergency Economic Powers Act ("IEEPA") authorizes sanctions against "property in which any foreign country or a national thereof has any interest." 50 U.S.C. § 1702(a)(1)(B). The North Korea Act ("NKA") permits sanctions against "property and interests in property" of "any person" who knowingly engages in certain conduct. 22 U.S.C. § 9214(c). It is the sole prerogative of Congress to expand these terms. Executive Orders 13722 and 13694 are based on the clear text of these statutes and authorize OFAC to sanction "persons" who have provided support to the North Korean government or engaged

in certain malicious cyber activities. 80 Fed. Reg. 18,077 (Apr. 1, 2015), *amended by* 82 Fed. Reg. 1 (Dec. 28, 2016); 81 Fed. Reg. 14,943 (Mar. 15, 2016).

As outlined below, these statutes do not contemplate the power to sanction open-source, decentralized, and ownerless software code because it is not "property." The district court's decision bypasses this inquiry entirely, in the process ignoring a critical prerequisite to OFAC designation. For its part, OFAC's suggestion that smart contracts constitute "property" distorts plain statutory text, and, if adopted, risks hamstringing socially beneficial innovation.

A review of dictionaries, as well as legal and historical precedent, provides sufficient reason to reject OFAC's conclusion that Tornado Cash smart contracts constitute "property." These sources share a common understanding of property: it must be capable of being owned. But certain Tornado Cash smart contracts are simply lines of code that are freely available for public viewing and cannot be owned.

Dictionaries have long defined "property" to include ownership. Samuel Johnson, for example, defined property broadly as "[r]ight of possession," "[p]ossession held in one's own right," and "[t]he thing possessed." 2 Samuel Johnson, *Dictionary of the English Language* (1755 ed.); *see also Black's Law Dictionary* 1095 (5th ed. 1979) ("everything which is or may be the subject of

ownership, whether a legal ownership, or whether beneficial, or a private ownership.").[17]

Legal precedent is the same. Although IEEPA and NKA do not define "property," the Supreme Court has described "property" as "all objects or rights which are susceptible of ownership." *Meyer v. United States*, 364 U.S. 410, 412 n.3 (1960). The Supreme Court also has explained that this concept of "property" comprises a "bundle of rights." *Dolan v. City of Tigard*, 512 U.S. 374, 384 (1994). And the "sticks" that make up that "bundle of rights" highlight the importance of ownership. For example, the "right to exclude others" is "one of the most essential sticks in the bundle of rights that are commonly characterized as property." *Kaiser Aetna v. United States*, 444 U.S. 164, 176 (1979).

Historical sources concur. President James Madison defined property as "that dominion which one man claims and exercises over the external things of the world, in exclusion of every other individual."[18] And English jurist William Blackstone famously defined property as "that sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the

---

17 *See, e.g.*, Property, Oxford English Dictionary (2d ed. 1989); Property, Webster's New World Dictionary of the American Language (college ed. 1968); Property, Webster's Third New International Dictionary (1961).

18 *Property, James Madison, Papers 14:266—68*, The University of Chicago Press, https://rb.gy/f493i (last visited Dec. 21, 2023).

right of any other individual in the universe."[19] Without ownership, there would be no property.

Fundamentally, it is simply not true that all of the sanctioned Tornado Cash smart contracts can be owned or operated. As described above, the core Tornado Cash smart contracts are immutable, autonomous, and self-executing open-source code that exist on the Ethereum blockchain. It has not been possible—from a technical perspective—to alter particular Tornado Cash smart contract pools since 2020. More specifically, these Tornado Cash smart contracts have explicit embedded code with an "_operator" variable that indicates the address of the entity that controls the contract. Prior to and at the time of OFAC's designation, the state of the operator was set to "0" for certain Tornado Cash smart contracts, meaning that the software code is *inalterable*. Indeed, because the code is set to "0," no person or entity will ever be able to alter these smart contract addresses or exert other control over them. In this way, the smart contracts function like an impenetrable safe after it has been locked and the only key destroyed.

Accordingly, upholding OFAC's designation of Tornado Cash smart contracts would fundamentally alter the definition of "property" that has stood for hundreds

---

[19] 2 William Blackstone, Commentaries on the Laws of England 2 (Univ. of Chicago Press 1979).

of years. Because no individual possesses a legitimate or practicable claim to exercise exclusive control over the lines of code that constitute ownerless Tornado Cash smart contracts, the smart contracts cannot constitute property. Courts have found that items to which individuals have no legitimate claim, or over which they do not exercise exclusive control, such as phone numbers, cannot constitute property. *See, e.g.*, *In re StarNet, Inc.*, 355 F.3d 634, 637 (7th Cir. 2004) ("No one has a property interest in a phone number."); *cf. In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1075 (N.D. Cal. 2012) ("personal information"—e.g., a user's location, zip code, and device identifier—is not property because it is not "an interest capable of precise definition" or "capable of exclusive possession or control"). OFAC's unprecedented and unilateral decision to add publicly available inalterable software code to the Specially Designated Nationals and Blocked Persons ("SDN") List cannot stand in the absence of express Congressional authorization.

Without any stated justification or reasoning, the district court excused the agency's dramatic departure from centuries-old understandings of "property." Indeed, the district court ignored the definition of "property" entirely. The court rejected the argument that OFAC's statutory authority encompasses only "property interests." *Coin Center v. Yellen*, No. 3:22cv20375-TKW-ZCB, 2023 WL 7121095, at *5 (N.D. Fla. Oct. 30, 2023). But instead of taking the statutory prerequisites to designation in turn—first considering whether Tornado Cash smart contracts are

"property" and, if so, whether a qualified person has an "interest" in the smart contracts—the district court read the antecedent "property" prong out of the statute and focused exclusively on the "interest" limb. *See id.* at *5–7.

With its decision, which effectively excuses OFAC from satisfying the statutory requirement that a subject of designation qualify as "property," the district court gave OFAC authority to expand the settled definition of "property" in a way that Congress did not authorize or contemplate. The resulting reverberations across industries risk disrupting the expectations of marketplace participants, who now must question their established understanding of which things fall within the ambit of OFAC's regulatory authority.

For example, under OFAC's interpretation as upheld by the district court, the United States could sanction any open-source email protocol—including SMTP, POP3, and IMAP—on the basis that any email communication's content has the potential to be a conduit for illegal activity. Similar to open-source Tornado Cash smart contracts, email protocols are freely available to the public and decentralized in terms of their management; in essence, the protocol operates autonomously for anyone to use. Users typically use email applications, like Gmail, Yahoo, and Hotmail to access these email protocols. And like the Tornado Cash smart contracts, users of email protocols do not have a "property interest" in the code because there is no legally enforceable right to use it or exclude others from using it. Under

OFAC's reasoning in this case, the government could designate and block access to email protocols regardless of the fact that (i) an open-source email protocol is simply a software tool open for use in any manner to any member of the public, and (ii) the majority of users of email view it as a necessity and do not use it for unlawful or malign purposes. Allowing OFAC to wield its authority as it has in this case could yield dangerous results and would run afoul of its statutory authority. OFAC's statutory interpretation as upheld by the district court lacks a limiting principle.

III. THE DISTRICT COURT'S RULING JEOPARDIZES IMPORTANT INTERESTS IN PRIVACY AND INNOVATION.

If allowed to stand, the district court's ruling poses the very real risk of thwarting law-abiding citizens' pursuit of financial privacy and chilling innovation in blockchain technology and beyond.

A. If Upheld, the District Court's Decision Would Undermine Appropriate Financial Privacy.

The district court's decision calls into question the foundation of cutting-edge efforts to safeguard privacy in everyday financial transactions and online activities.

1. Financial Privacy Is an Important Human Interest.

The ability to transact without fear of public exposure is an interest held dear among populations across the globe. Individuals who live in authoritarian regimes, for example, find value, safety, and protection in private financial transactions. Because their lives are more subject to government surveillance, control, and

oversight than non-authoritarian regimes, individuals who undertake public transactions in these countries are subject to real risks of harm. Crypto affords these individuals the ability to financially support unpopular causes, including, for instance, participation in "human rights activities" in otherwise hostile circumstances and the provision by Russian nationals of "donations to the Ukrainian war conflict" that contradict government orthodoxy, without revealing their identity.[20] Individuals living within the United States similarly hold strong interests in the right to financial privacy.[21] Private financial transactions, for example, offer U.S. citizens a means to exercise other fundamental rights, such as paying for healthcare or "exercis[ing] their constitutionally protected associational rights."[22] Thus, reducing or eliminating financial privacy hinders the ability of individuals to protect other rights granted to them.

---

[20] Brad Bourque, *The Crypto Wars and the Future of Financial Privacy*, Fordham J. of Corp. & Fin. L. (Mar. 31, 2023), https://news.law.fordham.edu/jcfl/2023/03/31/the-crypto-wars-and-the-future-of-financial-privacy/.

[21] The importance of financial privacy is not a novel concept in the United States For instance, the Right to Financial Privacy Act of 1978 protects the confidentiality of personal financial records by creating a statutory Fourth Amendment protection for bank records. *See* 12 U.S.C. §§ 3401-3423.

[22] Bourque, *supra* n. 20.

Before the modern-day proliferation of the Internet, financial transactions between parties enjoyed measures of privacy generally not seen today. For example, cash transactions conducted outside of financial intermediaries such as banks and other reporting-obliged entities offer such privacy and anonymity. But as individuals have moved from transacting in physical cash to transacting digitally online, the same privacy protections that individuals once took for granted no longer exist. Indeed, "[d]ata brokers have created a marketplace for exchanging information about individuals that can be used to link their various online actions" to determine "the history of activities associated with any given individual person."[23] As a result, "[t]he risk to consumers increases with the ever-increasing share of financial transactions that are performed electronically."[24] It is, therefore, no surprise that certain segments of our society have sought to reclaim financial privacy.

2. Blockchain Implicates Significant Privacy Concerns.

The ease with which crypto asset address pseudonymity can be overcome is a significant challenge for the future of blockchains. At the same time that blockchains facilitate technological innovation, they create a major paradox in

---

[23] Geoff Goodell & Tomaso Aste, *Can Cryptocurrencies Preserve Privacy and Comply with Regulations*, Frontiers in Blockchain (May 28, 2019), https://www.frontiersin.org/articles/10.3389/fbloc.2019.00004/full.

[24] *Id.*

privacy. Participants in blockchain networks can trust the veracity of the information because they can see and verify the details themselves. But that same transparency poses a real threat to an individual's privacy, not to mention safety,[25] and may chill the use of this important technology. Users are disincentivized from moving their financial data on-chain if that means exposing that data to the entire world. The same concerns apply to non-financial data as well, such as private healthcare information and other deeply personal data.

In addition to the important privacy implications of having such sensitive data on-chain, there are other important risks that run the gamut in terms of severity. Take the instance of a mom-and-pop shop that accepts payment in cryptocurrency from its customers. The store's cashiers could access some of their customer's financial activity information—for example, where that customer shopped yesterday if that activity was conducted on-chain, or the customer's total crypto holdings on the respective blockchain network used for the transaction. Larger risks also abound for individuals conducting non-private blockchain transactions, including surveillance from bad actors, consumer scams, and other potentially harmful consequences. Former Supreme Court Justice William O. Douglas was prescient in stating that "[t]he right to be let alone is indeed the beginning of all freedom," as

---

[25] Gary Weinstein, *AI And Blockchain Analytics: The Urgent Need For Crypto Privacy Tools*, Forbes (Apr. 7, 2023), https://rb.gy/1si0l.

most Internet users will always value privacy over other benefits of blockchains. *Pub. Utilities Comm'n of D.C. v. Pollak*, 343 U.S. 451, 467 (1952) (Douglas, J., dissenting).

3. Tornado Cash Protects User Privacy.

Most important Internet applications could not exist without significant privacy protections for their users. Email, messaging, and banking applications, for example, depend on the confidential exchange of sensitive information and data. Few users would accept otherwise. If online banking applications exposed the contents of users' bank accounts to the world, the security of an untold number of users would be jeopardized, leaving future users reluctant to use online banking services. But transparency is currently the standard practice of most blockchain networks, such as Ethereum—the blockchain that underlies most Tornado Cash smart contracts.

It is precisely software tools like Tornado Cash that provide individuals with an alternative method of protecting their data, limit third-party access to their financial transactions, and place leverage and control back into the hands of the individual. Indeed, Tornado Cash reflects one of a series of "new encryption methods that will revolutionize our conceptions of financial privacy."[26]

---

[26] Bourque, *supra* n. 20.

Although the government has legitimate concerns about national security and preventing crime, privacy-preserving technologies keep users safe against various bad actors, such as people seeking to harass or "dox"[27] others, or criminals attempting to gain knowledge of an individual's financial footprint and holdings. Crypto and blockchain technology can serve as a "natural alternative for exchanging value that can avoid the watchful eye of state actors, powerful corporations, hackers, and others who might be well-positioned to build a dossier of one's activities."[28]

Unfortunately, the free rein that the district court afforded OFAC strikes at the very heart of these important efforts to safeguard privacy in crypto transactions.

B. If Upheld, the District Court's Ruling Risks Stifling Innovation.

The district court's extreme deference to OFAC, reflected in its disregard of the limitation of OFAC's designation authority to "property," has the very real potential to chill investment in and stagnate development of new technologies that otherwise could produce enormous societal benefits. If OFAC is given carte blanche to rewrite settled legal definitions in pursuit of its regulatory objectives, no company can feel certain that its investment in cutting-edge software will fall outside OFAC's

---

27 "Dox" means to "publicly identify or publish private information about (someone) especially as a form of punishment or revenge." *Dox*, Merriam-Webster.com Dictionary, https://rb.gy/62vv0 (last visited Dec. 21, 2023).

28 Goodell & Aste, *supra* n. 23.

reach. And this unpredictability will force companies to abandon product development for fear of guessing wrong and seeing their huge investments of time, money, and innovative intellectual efforts vanish overnight.

Indeed, OFAC designation carries severe and immediate consequences. "Experts have referred to IEEPA sanctions as a 'financial death sentence.'"[29] "[D]esignation is not a mere inconvenience or burden on certain property interests; designation indefinitely renders a domestic organization financially defunct." *Al Haramain Islamic Found., Inc. v. Dep't of Treasury*, 686 F.3d 965, 980 (9th Cir. 2012); *see also, e.g.*, *Fares v. Smith*, 901 F.3d 315, 323 (D.C. Cir. 2018) ("As a general matter, the effect of an OFAC designation on the designee's private interests is 'dire.'"). "In most cases, anyone who falls within the legal jurisdiction of the United States is barred from transacting with persons or entities designated as targets of sanctions, and any property of a target that comes within U.S. jurisdiction must be frozen."[30] Given the risk of a functional erasure of years of work and investment with minimal judicial oversight, companies might bypass development in new

---

29 Andrew Boyle, *Checking the President's Sanctions Powers: A Proposal to Reform the International Emergency Economic Powers Act*, Brennan Center for Justice (June 10, 2021).

30 *Id.*

software technologies targeted by OFAC in favor of safer—but potentially less socially beneficial—opportunities.

In this way, the consequences of the district court's ruling are at cross-purposes with the federal government's stance on innovation in the financial sector. The current Presidential administration has signaled its commitment to "foster[ing] responsible digital asset innovation," in keeping with the long-standing "U.S. government . . . role in priming responsible private-sector innovation" through "sponsor[ing] cutting-edge research, help[ing] firms compete globally, assist[ing] them with compliance, and work[ing] with them to mitigate harmful side-effects of technological advancement." [31] Similarly, the Treasury Department recently emphasized that "responsible innovation has been a motto for [the] Department" and rededicated itself to facilitating "[i]nnovation" as "a ladder, to help more people climb to a higher quality of life."[32] And officials at the Federal Reserve, too, have highlighted the concept of "responsible innovation, which recognizes the important

---

[31] *Fact Sheet: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets*, The White House (Sept. 16, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/.

[32] *U.S. Treasury Department Holds Financial Sector Innovation Policy Roundtable*, U.S. Dep't of Treasury (Feb. 10, 2021), https://home.treasury.gov/news/press-releases/jy0023.

role of private-sector innovation" and "focuses policymakers on thinking about payment and financial system infrastructure and effective policy."[33]

OFAC's shotgun approach to designation of critical software, and the district court's failure to carefully scrutinize that regulatory decision, thus risks stultifying the very types of innovation that a significant cross-section of federal policymakers deems singularly important.

---

[33] Gov. Michelle W. Bowman, *Responsible Innovation in Money and Payments*, Board of Governors of the Federal Reserve (Oct. 17, 2023) https://www.federalreserve.gov/newsevents/speech/bowman20231017a.htm.

CONCLUSION

For the foregoing reasons, amicus curiae Andreessen Horowitz respectfully requests that the Court reverse the judgment of the district court.

Dated: December 21, 2023

Respectfully submitted,

/s/ Alessio D. Evangelista
Alessio D. Evangelista
Jessie K. Liu
SKADDEN, ARPS, SLATE,
MEAGHER & FLOM LLP
1440 New York Avenue, N.W.
Washington, DC 20005
Telephone: (202) 371-7000
Fax: (202) 661-9170
alessio.evangelista@skadden.com
jessie.liu@skadden.com

Counsel for Amicus Curiae Andreessen Horowitz

CERTIFICATE OF COMPLIANCE

This document complies with the word limit of FRAP 29(a)(5) because, excluding the parts of the document exempted by FRAP 32(f), this document contains 5,803 words.

This document complies with the typeface requirements of FRAP 32(a)(5) and the type-style requirements of FRAP 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in Times New Roman font size 14.

/s/ Alessio D. Evangelista
Alessio D. Evangelista

Counsel for Amicus Curiae
Andreessen Horowitz

Dated: December 21, 2023